Template - January 30, 2009, Version 2

Department of Energy
Privacy Impact Assessment (PIA)

Affects Members Of the Public?

Mark if Applicable w/ an X

Guidance is provided in the template. See DOE Order 206.1, *Department of Energy Privacy Program,* Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA:
http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

Please complete electronically: no hand-written submissions will be accepted.

Module I – Privacy Needs Assessment		
Date	Date the assessment was completed.	
Departmental Element & Site	The official list of Departmental Elements can be accessed at www.directives.doe.gov/pdfs/reftools/org-list.pdf. Please also list the site-location of the system with as much specificity as possible (e.g. DOE Headquarters, Forrestal, 1G-053 server room).	
Name of Information System or IT Project	Enter the name of the information system. If the system is part of an enclave or general support system (GSS), please include the name of the enclave or GSS along with the name identifying the application or subsystem being assessed.	
Exhibit Project UID	Enter the project unique identifier used for capital planning (eCPIC) or the contract name that provides the funding for the system.	
	Name, Title	**Contact Information Phone, Email**
System Owner	System Owners are Departmental Element officials responsible for monitoring the information systems under their purview to ensure compliance with this Order. System Owners are responsible for the overall procurement, development, integration, maintenance, secure operation, and safeguarding of Privacy information including PII for their information system(s). System owners may be Federal or contractor employees.	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov

Module I – Privacy Needs Assessment

Privacy Act Officer	Privacy Act Officers or Privacy Points of Contact (PPoCs) are designated by the Head of the Departmental Element. PAOs and PPoCs advocate and promote Privacy program activities within their Departmental Elements, as well as advise and provide Privacy Act subject matter expertise to their Departmental Elements, specifically with regard to conducting PIAs and completing the SORN process.	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	System Owners must engage cyber security experts to review this assessment before submission. Each organization may have these responsibilities assigned a little differently, whether it be to Information System Security Officer (ISSO) or another cyber security professional.	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov
Person Completing this Document	Name and title of the person(s) completing this document.	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov
Purpose of Information System or IT Project	Describe the purpose of this system, specifically as it relates to the organization's mission. For example, "The Acuity system is by DOE Headquarters to process employee payroll for Federal employees." Please provide a sufficient level of detail to cover all purposes of the system. This information is included when submitting a narrative statement to OMB and Congress for new and major amendments to Privacy Act Systems of Records. It also is included in the Privacy Act Systems of Records Notice (SORN) published in the Federal Register. If the system has a SORN, the response to this question should reflect the information in the narrative and notice.	

Module I – Privacy Needs Assessment

Type of Information Collected or Maintained by the System:	□ SSN Social Security number □ Medical & Health Information e.g. blood test results □ Financial Information e.g. credit card number □ Clearance Information e.g. "Q" □ Biometric Information e.g. finger print, retinal scan □ Mother's Maiden Name □ DoB, Place of Birth □ Employment Information □ Criminal History □ Name, Phone, Address □ Other – Please Specify
Has there been any attempt to verify Information about an Individual in Identifiable Form does not exist on the system? ***OMB 03-22 defines Information in identifiable form*** as information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).	YES or NO Some systems employ software tools to scan content (information or data) to search for types of data such as Social Security numbers.
If "Yes," what method was used to verify the system did not contain Information in Identifiable Form? (e.g. system scan)	Name the tools, processes (what types of information is scanned and scanned for) and frequency of the scanning.

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES or NO
2. Is the information in identifiable form?	YES or NO

Module I – Privacy Needs Assessment

3. Is the information about individual members of the public?	YES or NO
4. Is the information about DOE or contractor employees?	YES or NO

If the answer to the **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

For information systems that collect, maintain or disseminate information in identifiable form from or about members of the public, please complete Modules II and III. Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. This template may not be modified. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II (and III if necessary).

Module II – System Information for All Systems

1. What categories of individuals are collected or maintained by the information system?	□ Federal Employees □ Contractor Employees □ Members of the Public Individuals in non-employee or contractor context. This includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE. □ Other, Please Specify

Module II – System Information for All Systems

2. What is the source(s) of information about individuals in the information system?	For example, individual-provided; other Federal agency; tribal, state or local government entity; named third party, other (please identify). A third party is usually a non-Federal person or entity, who may be a source of data/information (e.g. informant, an internet service provider, a neighbor or friend, etc).
3. With what other agencies or entities will an individual's information be shared? How will the information be used?	Name of the Federal agency; tribal, state or local government entity; named third party.
4. Is the use of the information in identifiable form both relevant and necessary for the mission of the organization and DOE?	Describe how the information is used to accomplish a stated purpose of the agency and organization. For example, clearance information may be collected in support of the agency's national security mission.
5. Are the data elements described in detail and documented?	Is there a document that describes the data elements? E.g., a database schema that describes the elements and shows the data relationships?
REPORTS	
6. What kinds of reports are produced about individuals or that contain an individual's data?	For example, employee time and expense history.
7. What will be the use of these reports?	For example, the employee time and expense history may be used by the human resources department to manage payroll and reimbursement of expenses.
8. Who will have access to these reports?	Names and/or roles of individual(s) who will have access to these reports.
MAINTENANCE	
9. If the information system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	System Owners and information owners are responsible for ensuring information is used and managed consistently for its stated purpose in support of the organization. Please describe processes, procedures, software tools, etc. that are used to support this goal.
10. What are the retention periods of data in the information system?	Please describe policies, processes and procedures (if any) for retaining data in the system.

Module II – System Information for All Systems

11. What are the procedures for disposition of the data at the end of the retention period?	Please describe policies, processes and procedures (if any) for destroying data in the system, including paper reports, artifacts and other media that contain data which has reached the end of its retention period.
12. How does the use of this information system affect privacy? Consider also the use of emerging technologies and how those technologies may impact privacy.	Please describe how the use of this system and its technologies may impact an individual's privacy.
ACCESS	
13. What controls are in place to protect the data from unauthorized access, modification or use?	Please describe all security controls used to protect the system and its data from unauthorized access.
14. If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?	This question applies to systems in transition. If the data is being consolidated (i.e, combined or united into one system, application or process), the existing controls, if any, should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not accessed by someone unauthorized to access the data. Please describe management, operational and technical controls used to ensure safeguards are maintained while processes and technologies are consolidated.
15. Who will have access to this information system and its data (all data)? Will other agencies share data or have access to the data in this system? How will the data be used by the other agency?	Names and/or roles of individual(s) who will have access to this data.
16. Who will have access to information in identifiable form or and PII?	Names and/or roles of individual(s) who will have access to the PII data.
17. How is access to the data determined?	For example, will users have access to all data on the information system or will the user's access be restricted?

Module II – System Information for All Systems	
18. Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?	Answering this question typically requires checking with the contracts officer to ensure the requirements provided in the DOE Privacy Order Contractor Requirements Document are appropriately addressed in the contract(s).
19. Do other information systems share data or have access to the data in the system? If yes, explain.	Many information systems interconnect and share data. Please identify all systems that connect to and access information on this system.
20. For connecting information systems, is there an ISA other agreement between System Owners to ensure the privacy of individuals is protected?	Interconnection Security Agreements (ISA) outline the responsibilities and expectations associated with system interconnection. ISAs specify security requirements and controls necessary for interconnection and compliance.
21. Who is responsible for assuring proper use of the information system's information in identifiable form?	Names and/or roles of individual(s) who have this assigned responsibility.

Module III – Systems with Information About Members of the Public

1. What legal authority authorizes the purchase, development or maintenance of this information system?	What statutory provisions or Executive Order authorizes the collection and maintenance of the information to meet an official program mission or goal? This information is included when submitting a narrative statement to OMB and Congress for new and major amendments to Privacy Act Systems of Records. It also is included in the Privacy Act Systems of Records Notice (SORN) published in the Federal Register. If the system has a SORN, the response to this question should reflect the information in the narrative and notice.
2. Has a Privacy Act System of Records Notice been published in the Federal Register? If "Yes," provide name of SORN and location in the Federal Register.	The Privacy Act requires publication of a notice in the Federal Register describing each System of Records subject to the Act. Any officer of employee who knowingly and willfully maintains a System of Records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5,000. If a name or other personal identifier is not used to retrieve information, it is possible that the system is not a Privacy Act System of Records.
3. If the information system is being modified, will the SORN require amendment or revision?	YES or NO
4. How will data collected from sources other than DOE records be verified for accuracy, relevance and completeness?	The Privacy Act of 1974 requires that each agency that maintains a System of Records “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” (5 U.S.C. 552a (e)(5)). If the data does not meet any one of these components, fairness in making any determination is compromised. The information must have some form of verification for accuracy because of the Privacy Act provision that requires that only relevant and accurate records should be collected and maintained about individuals. Data accuracy and reliability are important requirements in implementing the Privacy Act. Data must also be complete before that the data is deemed accurate. Therefore, this section should state the steps the agency has taken to ensure the data is complete.

Module III – Systems with Information About Members of the Public

5. Are records in the system about individuals current? What steps or procedures are taken to ensure the data is current?	If the data is not current, then the relevancy and accuracy of the data are called into question. When possible, the data should be obtained from and/or verified with the individual to whom it pertains.
6. Will the information system derive new or meta data about an individual through aggregation from the information collected? How will this be maintained, including verified for relevance completeness, and accuracy?	What is meant by derived and aggregation? All enhanced or modernized systems most likely will derive new data and create previously unavailable data about an individual from the information collected through aggregation. Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information. Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data.
7. Will the new or meta data be part of an individual's record?	Will the information be placed in a new record or a record with existing information that pertains to the individual? If the information is placed in a file that pertains to the individual and is retrieved by a personal identifier, a Privacy Act System of Records must be established or amended.
8. How will the new or meta data be used? Will it be used to make determinations about members of the public?	Describe the use of the new or meta data.
9. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.	Data can be retrieved a number of ways, but there is usually a personal identifier associated with a data retrieval mechanism. A system with data on individuals that is retrieved by a name or personal identifier may constitute a Privacy Act System of Records and require a notice (or an amended notice) be published in the *Federal Register*.
10. What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only	Describe mechanisms and/or processes available for the individual to accept or decline the personal information being provided and if there are any penalties if the information is not provided.

Module III – Systems with Information About Members of the Public	
to particular uses of the information (other than required or authorized uses)?	
11. Will this information system provide the capability to identify, locate, and monitor individuals?	Identify any tracking and monitoring, including methods, of individuals to whom the information pertains.
12. What kinds of information are collected as a function of the monitoring of individuals?	Identify types of information collected. For example, Social Security numbers.
13. What controls will be used to prevent unauthorized monitoring?	Please describe all security controls used to protect the system and its data from unauthorized monitoring.

SIGNATURE PAGE

	Signature	Date
System Owner	______________________________ **(Print Name)** ______________________________ **(Signature)**	______________
Privacy Act Officer	______________________________ **(Print Name)** ______________________________ **(Signature)**	______________
Jerry Hanley **Chief Privacy Officer**	______________________________	______________
Ingrid Kolb **Senior Agency Official for Privacy (SAOP)**	______________________________	______________